APPENDIX A – ASSERTED CLAIMS WITH DISPUTED TERMS SHOWN IN BOLD

079 Patent

1. An authentication system for authenticating the identity of a requester of access by an **unauthorized service client** to a **secured resource**, said authentication system comprising:

a **messaging gateway** having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an **authorized user** of a **secured resource** a request for access by an **unauthorized service client** to said **secured resource**;

a server in secure communication with said **messaging gateway**, said server having a second set of instructions embodied in a computer readable medium operable to determine a **key string known to both said secured resource and the authorized user** said requestor purports to be, said **key string being adapted to provide a basis for authenticating the identity of said requester**;

a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said **unauthorized service client**;

wherein said second set of instructions is further operable to receive an **authentication credential** from said **unauthorized service client** associated with said request for access, said **authentication credential** having been provided to said **unauthorized service client** by said requestor; and

wherein said second set of instructions is further operable to evaluate said **authentication credential** to authenticate the identity of said requester.

2. The authentication system as recited in claim 1 wherein:

said second set of instructions is further operable to generate a confirmation message indicating receipt of said request for access; and

said first set of instructions is further operable to communicate said confirmation message to said **authorized user** that said requester purports to be.

3. The authentication system as recited in claim 1 wherein said second set of instructions is further operable to for determine from among a plurality of **secured resources** associated with said **authorized user** the identity of a single **secured resource** to which said requester requests access.

6. The authentication system as recited in claim 1, wherein said second set of instructions includes instructions operable to invalidate said **authentication credential based upon passage of time**.

7. The authentication system as recited in claim 1, said second set of instructions operable to conduct for the benefit of said **unauthorized service client** a transaction reliant upon access to said **secured resource**.

8. The authentication system as recited in claim 7, said second set of instructions further operable to:

generate a receipt for said transaction; and

transmit said receipt to said **authorized user**.

9. The authentication system as recited in claim 7, wherein said transaction comprises providing a financial benefit.

11. A method for authenticating the identity of a requester of access to a **secured resource**, said method for authenticating comprising the steps of:

receiving at a **messaging gateway** having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an **authorized user** of a **secured resource**, a request for access by an **unauthorized service client** to a **secured resource** from a requester purporting to be an **authorized user** of said **secured resource**;

determining a **key string** with a server in secure communication with said **messaging gateway**, said server having a second set of instructions embodied in a computer readable medium operable to determine a **key string known to both said secured resource and the authorized user** said requestor purports to be, said **key string being adapted to provide a basis for authenticating the identity of said requester**;

a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client;

wherein said second set of instructions is further operable to receive from said **unauthorized service client** an **authentication credential** associated with said request for access, said

authentication credential having been provided to said **unauthorized service client** by said requestor; and

wherein said second set of instructions is further operable for evaluating said **authentication credential** to authenticate the identity of said requester.

12. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 11, said method for authenticating further comprising the steps of:

generating a confirmation message indicating receipt of said request for access; and

communicating said confirmation message to said **authorized user** that said requester purports to be.

13. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 11, said method for authenticating further comprising the step of determining from among a plurality of **secured resources** associated with said **authorized user** the identity of a single **secured resource** to which said requester requests access.

16. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 11, said method for authenticating further comprising the step of determining **based upon passage of time** whether said **authentication credential** should be deemed invalid.

17. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 11, said method for authenticating further comprising the step of conducting for the benefit of said **unauthorized service client** a transaction reliant upon access to said **secured resource**.

18. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 17, said method for authenticating further comprising the steps of:

generating a receipt for said transaction; and

transmitting said receipt to said **authorized user**.

19. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 17, wherein said transaction comprises providing a financial benefit.

802 Patent

1. An authentication system for authenticating the identity of a requester of access by an **unauthorized service client** to a **secured resource**, said authentication system comprising:

a **messaging gateway** having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an **authorized user** of a **secured resource** a request for access by an **unauthorized service client** to said **secured resource**;

a server in secure communication with said **messaging gateway**, said server having a second set of instructions embodied in a computer readable medium operable to generate a **key string adapted to provide a basis for authenticating the identity of said requester**;

a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said **unauthorized service client**;

wherein said first set of instructions is further operable to communicate said **key string** to said **authorized user** that said requester purports to be;

wherein said second set of instructions is further operable to receive an **authentication credential** from said **unauthorized service client**, said **authentication credential** having been provided to said **unauthorized service client** by said requester; and

wherein said second set of instructions is further operable to evaluate said **authentication credential** to authenticate the identity of said requester.

2. The authentication system as recited in claim 1 wherein said second set of instructions is further operable to determine from among a plurality of **secured resources** associated with said **authorized user** the identity of a single **secured resource** to which said requester requests access.

5. The authentication system as recited in claim 2, wherein said second set of instructions further is operable to generate a plurality of **key strings**, each one of said plurality of **key strings** being associated with a single one of said plurality of said **secured resources**.

6. The authentication system as recited in claim 1, wherein said second set of instructions includes instructions operable to invalidate said **authentication credential based upon passage of time**.

7. The authentication system as recited in claim 1, second set of instructions operable to conduct for the benefit of said **unauthorized service client** a transaction reliant upon access to said **secured resource**.

8. The authentication system as recited in claim 7, said second set of instructions further operable to:

generating a receipt for said transaction; and

transmitting said receipt to said **authorized user**.

9. The authentication system as recited in claim 7, wherein said transaction comprises providing a financial benefit.

11. A method for authenticating the identity of a requester of access to a **secured resource**, said method for authenticating comprising the steps of:

receiving at a **messaging gateway** having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an **authorized user** of a **secured resource**, a request for access by an **unauthorized service client** to a **secured resource** from a requester purporting to be an **authorized user** of said **secured resource**;

generating a **key string** with a server in secure communication with said **messaging gateway**, said server having a second set of instructions embodied in a computer readable medium operable to generate a **key string adapted to provide a basis for authenticating the identity of said requester**;

a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client;

wherein said first set of instructions is further operable to communicate said **key string** to said **authorized user** that said requester purports to be;

wherein said second set of instructions is further operable to receive an **authentication credential** from said **unauthorized service client**, said **authentication credential** having been provided to said **unauthorized service client** by said requester; and

wherein said second set of instructions is further operable to evaluate said **authentication credential** to authenticate the identity of said requester.

12. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 11, said method for authenticating further comprising the step of determining from among a plurality of **secured resources** associated with said **authorized user** the identity of a single **secured resource** to which said requester requests access.

16. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 11, said method for authenticating further comprising the step of determining **based upon passage of time** whether said **authentication credential** should be deemed invalid.

17. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 11, said method for authenticating further comprising the step of conducting for the benefit of said **unauthorized service client** a transaction reliant upon access to said **secured resource**.

18. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 17, said method for authenticating further comprising the steps of:

generating a receipt for said transaction; and

transmitting said receipt to said **authorized user**.

19. The method for authenticating the identity of a requester of access to a **secured resource** as recited in claim 17, wherein said transaction comprises providing a financial benefit.

499 Patent

1. A method for authorizing transaction specific access to a **secured resource** having a **secured resource** identity, said method comprising the steps of:

receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client;

determining a **key string** with a server in communication with said **messaging gateway**, said server having a second set of instructions embodied in a computer readable medium operable to determine said **key string known to both said server and an authorized user** of said **secured resource**, said **key string** being associated with the **secured resource** identity within a **key string** table accessible by the server and providing a basis for authenticating the **secured resource** identity by searching the **key string** table for the **key string**;

determining transaction specific information with the server in communication with the **messaging gateway**, said server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request;

determining an **authentication credential** with the server in communication with said **messaging gateway**, the server having a fourth set of instructions operable to identify within the request an **authentication credential** uniquely associated with said transaction specific information and said **key string**, said **authentication credential** having been provided by the **authorized user**;

evaluating said **authentication credential** by the server, the server having a fifth set of instructions operable to compare the **key string** and the transaction specific information with the **authentication credential** to verify that the transaction specific access to the **secured resource** by the **service client** is authorized by the **authorized user**; and

wherein the **key string** and **authentication credential** do not reveal any **primary identifier** associated with said **secured resource**.

2. The method of claim 1 further comprising the step of communicating with a resource provider through a resource gateway in communication with the server.

3. A method for authorizing transaction specific access to a **secured resource** having a **secured resource** identity, said method comprising the steps of:

receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive a request for transaction specific access to a secured resource by a service client;

generating a **key string** with a server in communication with said **messaging gateway**, said server having a second set of instructions embodied in a computer readable medium operable to generate the **key string known to both said server and an authorized user** of said **secured resource**, said **key string** being associated with the **secured resource** within a **key string** table accessible by the server and providing a basis for authenticating the **secured resource** identity by searching the **key string** table for the **key string**;

determining transaction specific information with the server, the server having a third set of instructions embodied in a computer readable medium operable to identify transaction specific information within the request;

communicating said **key string** to said **authorized user**;

receiving an **authentication credential** from said **service client**, said **authentication credential** having been provided to said **service client** by said **authorized user**; and

evaluating said **authentication credential**; and

wherein the **key string** and **authentication credential** do not reveal any **primary identifier** associated with said **secured resource**.

<u>659 Patent</u>

1. A computer-implemented method for a credit or debit card account holder to authorize a resource provider to use a credit or debit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant, the computer-implemented method comprising the steps of:

providing at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both;

receiving registration information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same;

receiving an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising:

a first merchant identifier;

a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier;

the credit or debit card account holder identifier; and

a designated unique account identifier selected from the at least one unique account identifiers; and

generating a first transaction specific **authentication credential** associated with the authorization request, whereby the first transaction specific **authentication credential** comprises a **key string** wherein the **key string** is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier;

receiving a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising:

a second merchant identifier;

a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and a second transaction specific **authentication credential** whereby the second **authentication credential** was received by the merchant application from the credit or debit card account holder's mobile device; and

validating the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorizing the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the specific merchant by determining that:

the first merchant identifier matches the second merchant identifier;

the first transaction specific information matches the second transaction specific information; and

the first transaction specific **authentication credential** matches the second transaction specific **authentication credential**.

3. The computer-implemented authentication method of claim 1 further comprising the steps of storing the first transaction specific **authentication credential** for the authorization request message.

5. The computer-implemented authentication method of claim 1 further comprising the steps of completing the payment process using the credit or debit card account number for the designated unique account identifier without transmitting or otherwise providing the credit or debit card account number to the merchant.

6. The computer-implemented authentication method of claim 1 wherein the validation step must take place within a given time period.

7. The computer-implemented authentication method of claim 1 further comprising the step of determining whether the second **authentication credential** should be deemed invalid **based upon passage of time**.

9. A computer-implemented system for a credit or debit card account holder to authorize a resource provider to use a credit or debit card account number to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or debit card account number to the merchant, the computer-implemented system comprising:

at least one interface adapted to receive and transmit data in communication with a credit or debit card account holder's mobile device, a merchant's payment application, or both;

one or more servers in secure communication with the at least one interface, the one or more servers having:

a first instruction embodied in a computer readable medium, the first instruction operable to receive registration information received from the credit or debit card account holder through the at least one interface, the registration information comprising a credit or debit card account holder identifier and at least one credit or debit card account number having an associated unique account identifier wherein the credit or debit card account number and unique account identifier are not the same;

a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to pay the specific merchant for the specific transaction from a given debit or credit card account, the authorization request message having been received through the at least one interface and originating from the credit or debit card account holder's mobile device and comprising:

a first merchant identifier;

a first transaction specific information selected from the group consisting of a first transaction amount and first client reference identifier;

the credit or debit card account holder identifier; and

a designated unique account identifier selected from the at least one unique account identifiers; and

a third instruction embodied in a computer readable medium, the third instruction operable to:

generate a first transaction specific **authentication credential** associated with the authorization request, whereby the first transaction specific **authentication credential** comprises a **key string** wherein the **key string** is not a temporary credit or debit card account number and does not include or reveal the credit or debit card account number associated with the designated unique account identifier;

receive a payment request message from the merchant's payment application through the at least one interface, the payment request message comprising:

a second merchant identifier;

a second transaction specific information selected from the group consisting of a second transaction amount and second client reference identifier; and

a second transaction specific **authentication credential** whereby the second **authentication credential** was received by the merchant application from the credit or debit card account holder's mobile device; and validate the credit or debit card account holder's request to use the credit or debit card account number associated with the designated unique account identifier for payment to the specific merchant for the specific transaction and authorize the resource provider to use the credit or debit card account number associated with the designated unique account identifier to pay a specific merchant for a specific transaction without transmitting or otherwise providing the credit or bank account number to the specific merchant by determining if:

the first merchant identifier matches the second merchant identifier;

the first transaction specific information matches the second transaction specific information; and

the first transaction specific **authentication credential** matches the second transaction specific **authentication credential**.

11. The computer-implemented authentication system of claim 9 wherein the third instruction is further operable to store the first transaction specific **authentication credential** for the authorization request message.

13. The computer-implemented authentication system of claim 9 wherein the third instruction is further operable to complete the payment process using the credit or debit card account number for the designated unique account identifier without transmitting or otherwise providing the credit or debit card account number to the merchant.

14. The computer-implemented authentication system of claim 9 wherein the validation step must take place within a given time period.

15. The computer-implemented authentication system of claim 9 wherein the third instruction is further operable to determine whether the second **authentication credential** should be deemed invalid **based upon passage of time**.

454 Patent

1. A computer-implemented method for a user to authorize a **service client's** access to a **secured resource** associated with a **common identifier** without transmitting or otherwise providing the **secured resource's common identifier** to the **service client**, the computer-implemented method comprising the steps of:

providing at least one interface adapted to receive and transmit data in communication with a user's application, a **service client's** application, or both;

receiving registration information received from the user through the at least one interface, the registration information comprising a user identifier and at least one **secured resource** identifier associated with the **common identifier** of the **secured resource**, wherein the **common identifier** and the **secured resource** identifier are not the same;

receiving an authorization request message to authorize access to the **secured resource** by the **service client**, the authorization request message having been received through the at least one interface from the user's application and comprising:

a first **service client** identifier;

a first transaction specific information;

the user identifier; and

a designated **secured resource** identifier selected from one of the at least one **secured resource** identifiers; and

generating a first transaction specific **authentication credential** associated with the authorization request, whereby the first transaction specific **authentication credential** comprises a **key string** and does not include or reveal the **common identifier** associated with the designated **secured resource** identifier;

receiving an access request message from the **service client's** application through the at least one interface, the access request message comprising:

a second **service client** identifier; a second transaction specific information; and a second transaction specific **authentication credential** whereby the second transaction specific **authentication credential** was received by the **service client**'s application from the user's application; and

validating the user's request to access the **secured resource** associated with the designated **secured resource** identifier without transmitting or otherwise providing the **common identifier** of the **secured resource** to the **service client** by determining if:

the first **service client** identifier matches the second **service client** identifier;

the first transaction specific information matches the second transaction specific information; and

the first transaction specific **authentication credential** matches the second transaction specific **authentication credential**.

3. The computer-implemented authentication method of claim 1 further comprising the steps of storing the first transaction specific **authentication credential** for the authorization request message.

5. The computer-implemented authentication method of claim 1 further comprising the steps granting access to the **secured resource** associated with the designated **secured resource** identifier without transmitting or otherwise providing the **common identifier** of the **secured resource** to the **service client**.

6. The computer-implemented authentication method of claim 1 wherein the validation step must take place within a given time period.

7. The computer-implemented authentication method of claim 1 further comprising the steps determining whether the second transaction specific **authentication credential** should be deemed invalid **based upon passage of time**.

8. A computer-implemented system for a user to authorize a **service client's** access to a **secured resource** associated with a **common identifier** without transmitting or otherwise providing the **secured resource's common identifier** to the **service client**, the computer-implemented system comprising:

at least one interface adapted to receive and transmit data in communication with a user's application, a **service client's** application, or both;

one or more servers in secure communication with the at least one interface, the one or more servers having:

a first instruction embodied in a computer readable medium, the first instruction operable to receive registration information received from the user through at least one interface, the registration information comprising a user identifier and at least one **secured resource** identifier associated with the **common identifier** of the **secured resource**, wherein the **common identifier** and **secured resource** identifier are not the same;

a second instruction embodied in a computer readable medium, the second instruction operable to receive an authorization request message to authorize access to the **secured resource** by the **service client**, the authorization request message having been received through the at least one interface from the user's application and comprising:

a first **service client** identifier;

a first transaction specific information;

the user identifier; and

a designated **secured resource** identifier selected from one of the at least one **secured resource** identifiers; and

a third instruction embodied in a computer readable medium, the third instruction operable to:

generate a first transaction specific **authentication credential** associated with the authorization request, whereby the first transaction specific **authentication credential** comprises a **key string** and does not include or reveal the **common identifier** associated with the designated **secured resource** identifier;

receive an access request message from the **service client's** application through the at least one interface, the access request message comprising:

a second **service client** identifier;

a second transaction specific information; and

a second transaction specific **authentication credential** whereby the second transaction specific **authentication credential** was received by the **service client's** application from the user's application; and

validate the user's request to access the **secured resource** associated with the designated **secured resource** identifier without transmitting or otherwise providing the **common identifier** of the **secured resource** to the **service client** by determining if:

the first **service client** identifier matches the second **service client** identifier;

the first transaction specific information matches the second transaction specific information; and

the first transaction specific **authentication credential** matches the second transaction specific **authentication credential**.

10. The computer-implemented authentication system of claim 8 wherein the third instruction is further operable to store the first transaction specific **authentication credential** for the authorization request message.

12. The computer-implemented authentication system of claim 8 wherein the third instruction is further operable to grant access to the **secured resource** associated with the designated **secured resource** identifier without transmitting or otherwise providing the **common identifier** of the **secured resource** to the **service client**.

13. The computer-implemented authentication system of claim 8 wherein the validation step must take place within a given time period.

14. The computer-implemented authentication system of claim 8 wherein the third instruction is further operable to determine whether the second transaction specific **authentication credential** should be deemed invalid **based upon passage of time**.